

SUMS OF DILATES IN ORDERED GROUPS

ALAIN PLAGNE AND SALVATORE TRINGALI

ABSTRACT. We address the “sums of dilates problem” by looking for non-trivial lower bounds on sumsets of the form $k \cdot X + l \cdot X$, where k and l are non-zero integers and X is a subset of a possibly non-abelian group G (written additively). In particular, we investigate the extension of some results so far known only for the integers to the context of torsion-free or linearly orderable groups, either abelian or not.

1. INTRODUCTION

One of the main problems in additive combinatorics is to derive non-trivial bounds on the cardinality of *Minkowski sumsets* (usually called just sumsets), see [22, Chapter 1] for the basic terminology and notation. In this respect, the inequality:

$$|X + Y| \geq |X| + |Y| - 1, \quad (1)$$

where X and Y are non-empty subsets of the additive group of the integers, serves as a cornerstone and suggests at least two possible directions of research:

- (i) extending (1) to broader contexts, e.g. more general groups or possibly non-cancellative semigroups (abelian or not), see [30] and references therein;
- (ii) improving (1) for special pairs of sets (X, Y) .

Having this in mind, let G be a fixed group, which needs not be abelian, but we write additively (unless a statement to the contrary is made). For X a subset of G and k an integer, we define

$$k \cdot X = \{kx : x \in X\},$$

and we call $k \cdot X$ a *dilate* of X (we use $X^{\cdot k}$ in place of $k \cdot X$ when G is written multiplicatively).

The present paper is focused on some aspects of the following problem, which we refer to as the *sums of dilates problem*: Given integers k and l , find the minimal

2010 *Mathematics Subject Classification*. Primary 11P70; Secondary 11B25, 11B30, 11B75, 20F60.

Key words and phrases. Additive combinatorics, sum of dilates, Minkowski sumsets, linearly orderable group.

This research was supported by the French ANR Project “CAESAR” No. ANR-12-BS01-0011.

possible cardinality of a sumset of the form $k \cdot X + l \cdot X$ in terms of the cardinality of X or, equivalently, find a best possible lower bound for $|k \cdot X + l \cdot X|$. As far as we are aware, the study of this problem started about a decade ago, and until recent years it was mainly concerned with the case of $(\mathbb{Z}, +)$.

Specifically, early contributions to this subject date back at least to 2002, when Hamidoune and the first-named author obtained, as a by-product of an extension of Freiman's $3k - 3$ theorem, the following elementary estimate, valid for any non-empty set $X \subseteq \mathbb{Z}$ and any integer k with $|k| \geq 2$, see [14] and references therein:

$$|X + k \cdot X| \geq 3|X| - 2. \quad (2)$$

This result was refined by Nathanson [23], who showed that

$$|k \cdot X + l \cdot X| \geq \frac{7}{2}|X| - 3 \quad (3)$$

for any pair of positive coprime integers (k, l) , at least one of which is ≥ 3 . Notice here that there is no loss of generality in assuming that k and l are coprime, since replacing X with a set of the form $a \cdot X + b$, where a and b are integers and $a \neq 0$, does not change the cardinality of the left- and right-hand sides of (3).

The case $(k, l) = (1, 3)$ was then completely settled in [7] by Cilleruelo, Silva and Vinuesa, who established that

$$|X + 3 \cdot X| \geq 4|X| - 4, \quad (4)$$

and determined the cases in which (4) is an equality. In the same paper, the authors prove the inverse theorem that $|X + 2 \cdot X| = 3|X| - 2$ holds if and only if X is an arithmetic progression.

On another hand, the general problem of estimating the size of a sum of any finite number of dilates was considered in 2007 by Bukh [5], who showed that

$$|k_1 \cdot X + \cdots + k_n \cdot X| \geq (|k_1| + \cdots + |k_n|)|X| - o(|X|) \quad (5)$$

for any non-empty set $X \subseteq \mathbb{Z}$ and coprime integers k_1, \dots, k_n . It has been since then conjectured that the bound (5) can be actually improved to the effect of replacing the term $o(|X|)$ with an absolute constant depending only on k_1, \dots, k_n .

Together with applications of Bukh's results to the study of sum-product phenomena in finite fields [13], the above has motivated an increasing interest in the topic and led to a number of publications. In particular, Cilleruelo, Hamidoune and Serra proved in [6] that if k is a (positive) prime and $|X| \geq 3(k-1)^3(k-2)!$ then

$$|X + k \cdot X| \geq (1+k)|X| - \left\lceil \frac{k(k+2)}{4} \right\rceil, \quad (6)$$

and they also determined all cases where (6) holds as an equality. This in turn supports the conjecture, first suggested in [7], that (6) is true for any positive integer

k , provided that $|X|$ is sufficiently large. Likewise, Hamidoune and Rué showed in [15] that $|2 \cdot X + k \cdot X| \geq (2+k)|X| - 4k^{k-1}$ if k is again a prime, and in fact

$$|2 \cdot X + k \cdot X| \geq (2+k)|X| - k^2 - k + 2$$

if $|X| > 8k^k$.

In cases where the previous bounds do not apply, weaker but nontrivial estimates can however be obtained. For instance, Freiman, Herzog, Longobardi, Maj and Stanchescu [11] have recently improved (4) by establishing that

$$|X + k \cdot X| \geq 4|X| - 4$$

for any $k \geq 3$. In the same paper, the authors prove various direct and inverse theorems on sums of dilates in the integers which they use to obtain direct and inverse theorems for sumsets in certain submonoids of Baumslag-Solitar groups [4], that is two-generator one-relator groups defined by a presentation of the form

$$\langle a, b \mid ba^mb^{-1} = a^n \rangle,$$

where m and n are non-zero integers (throughout, as is usual, these and other finitely presented groups are written multiplicatively).

Finally, even more recently, the case of $(\mathbb{Z}, +)$ was almost completely settled by Balog and Shakan in [1], where it is proved that

$$|k \cdot X + l \cdot X| \geq (k+l)|X| - (kl)^{(k+l-3)(k+l)+1}$$

whenever k and l are coprime positive integers. Another preprint by Shakan [29] gives, in particular, an extension of this result (where the ‘error term’ on the right-hand side is a constant) to the case studied by Bukh of a general sum of dilates of the form $k_1 \cdot X + \dots + k_n \cdot X$ for which the coefficients k_i are positive integers and for $2 \leq j \leq n$ there exists an index $1 \leq i < j$ such that $\gcd(k_i, k_j) = 1$.

On another hand, as appears from the above historical overview (which is almost exhaustive), very little has been done so far with regard to the problem of providing non-trivial estimates for sums of dilates in groups different from $(\mathbb{Z}, +)$, especially if non-abelian. A couple of exceptions are two recent papers focused on the case of cyclic groups of prime order, namely [25] and [26], some results by Konyagin and Laba (see Section 3 of [19]) on sets of small doubling in linear spaces over the real or the rational field, and a 2014 preprint by Balog and Shakan [2] on sums of dilates in $(\mathbb{Z}^n, +)$.

The present article fits in this context and investigates some questions related to the extension of the inequality (2) to the setting of torsion-free or linearly orderable groups, either abelian or not.

2. GOING BEYOND THE INTEGERS

We say that an (additively written) group G is *linearly orderable* if there exists a total order \preceq on G such that $x + y \prec x + z$ and $y + x \prec z + x$ for all $x, y, z \in G$ with $y \prec z$, in which case we refer to \preceq as a linear order on G and to the pair (G, \preceq) as a linearly ordered group.

Linearly orderable groups form a natural class of groups for the type of problems studied in this article. E.g., they were considered by Freiman, Herzog, Longobardi and Maj in [10] in reference to an extension of Freiman's $3k - 3$ theorem, and some of their results were subsequently generalized by the second-named author to the case of linearly orderable semigroups [31].

In continuation to [10], Freiman, Herzog, Longobardi, Maj, Stanchescu and the first-named author have recently obtained, see [12], several new results on the structure of the subgroup generated by a small doubling subset of an ordered group (abelian or not), together with various generalizations of Freiman's $3k - 3$ and $3k - 2$ theorems.

The class of linearly orderable groups is closed under embeddings and direct products, and it notably includes torsion-free nilpotent groups (and so, in particular, abelian torsion-free groups), as established by Iwasawa [17], Malcev [21] and Neumann [24]; pure braid groups [28]; and free groups [17].

In the present context, linearly orderable groups serve as a basic generalization of the additive group of the integers, in that (1) and its proof (which is essentially based on the order structure of \mathbb{Z}) can be immediately transposed. Indeed, if G is a linearly orderable group and X and Y are non-empty subsets of G , then

$$|X + Y| \geq |X| + |Y| - 1. \quad (7)$$

In fact, we know even more since Kemperman proved [18] that (7) remains true if the ambient group is only supposed to be torsion-free. In particular, if k and l are non-zero integers and X is a non-empty subset of a torsion-free (and in particular linearly orderable) group, then

$$|k \cdot X + l \cdot X| \geq 2|X| - 1. \quad (8)$$

Based on this, we have the following result, which counts as an elementary generalization of (2) and serves as a starting point for the present work.

Theorem 1. *Let G be a torsion-free abelian group and X be a non-empty finite subset of G . Let k and l be non-zero integers with distinct absolute values. Then $|k \cdot X + l \cdot X| \geq 3|X| - 2$.*

Proof. Without loss of generality we assume that $|l| > |k| \geq 1$, in particular $|l| \geq 2$. In the case when $|X| = 1$, the result is immediate, so let $|X| \geq 2$ and define

$$k' = \frac{k}{\gcd(k, l)} \quad \text{and} \quad l' = \frac{l}{\gcd(k, l)}.$$

Clearly, k' and l' are non-zero integers with distinct absolute values and, G being abelian, we have

$$|k \cdot X + l \cdot X| = |k' \cdot (X - g) + l' \cdot (X - g)|$$

for every $g \in G$. Therefore, we can assume without loss of generality that 0 belongs to X , and k and l are coprime.

Furthermore, since X is finite and G is abelian and torsion-free, the subgroup of G generated by X is isomorphic to some finite power of $(\mathbb{Z}, +)$. Hence, we can as well suppose that X generates $G = (\mathbb{Z}^n, +)$ for some integer $n \geq 1$. We may thus define the greatest common divisor of X , which is by definition the greatest common divisor of the coordinates of the elements of $X \subseteq \mathbb{Z}^n$. If $d = \gcd X$, we obtain $X \subseteq (d \cdot \mathbb{Z})^n$. This implies $\mathbb{Z}^n = \langle X \rangle \subseteq (d \cdot \mathbb{Z})^n$ and thus $d = 1$.

Let now H be the subgroup of G generated by $l \cdot X$. One has $H = \langle l \cdot X \rangle \subseteq (l \cdot \mathbb{Z})^n$. We may decompose $k \cdot X$ into its non-empty intersections with cosets modulo H . Let $g_1, \dots, g_q \in G$ be such that the cosets $g_1 + H, \dots, g_q + H$ are pairwise disjoint and the intersection K_i of $k \cdot X$ with $g_i + H$ is non-empty. We obtain a partition of $k \cdot X$ in the form

$$k \cdot X = \bigcup_{i=1}^q K_i.$$

From this, we infer

$$|k \cdot X + l \cdot X| = \sum_{i=1}^q |K_i + l \cdot X|. \quad (9)$$

On another hand, since G is supposed to be equal to $(\mathbb{Z}^n, +)$, it is linearly orderable (e.g., by the natural lexicographic order induced by the usual order of the integers). So, we get from (8) and (9) that

$$|k \cdot X + l \cdot X| \geq \sum_{i=1}^q (|K_i| + |X| - 1) = (q + 1)|X| - q. \quad (10)$$

Suppose that $q = 1$. Since $0 \in X$, we would obtain $k \cdot X \subseteq H \subseteq (l \cdot \mathbb{Z})^n$. However, since $\gcd(k, l) = 1$, this would imply that X itself is included in $(l \cdot \mathbb{Z})^n$ which in turn gives that l divides $\gcd X = 1$ and finally $|l| = 1$, a contradiction. Thus we must have $q \geq 2$, and (10) implies the claim. \square

It is natural to ask if Theorem 1 continues to hold even without the assumption that the ambient group is abelian, and our next theorem shows that the answer to this question is negative. Note that from this point on, unless a statement to the contrary is made, we write groups multiplicatively whenever they are non-abelian.

Theorem 2. *Let k and l be non-zero integers. There exist a torsion-free group G and a 2-element subset X of G such that $|X^k X^l| < 3|X| - 2$.*

Later on, we will discuss the extension of this result to a 3-element larger X , but it seems extremely difficult to understand if this can be pushed further.

Nonabelian torsion-free groups are generally believed to enjoy better isoperimetric inequalities than the abelian ones. There is, for instance, a conjecture by Freiman stating that the inequality $|2X| < 3|X| - 4$ for a subset in a torsion-free group implies that the subgroup generated by X is cyclic (and then the structure of X can be recovered by Freiman's $3k - 4$ theorem). To our knowledge, the best general inequality for torsion-free groups can be found in [3], where the main result implies that, for any constant k one has $|2X| \geq 2|X| + k$ provided that $|X|$ is large enough and not contained in a coset of a cyclic subgroup.

This may indicate that small sets are precisely not the ones where good estimates will be found. However, an explicit example is given in [3] where

$$|X^2| = \frac{10}{3}|X| - \frac{13}{3},$$

which does not exclude finding arbitrarily large sets X with $|X^k X^l| < 3|X| - 2$ in torsion-free groups.

Proof of Theorem 2. If $k = -l$, then the claim is straightforward by taking G equal to the free group on the set $\{a, b\}$ and $X = \{a, b\}$.

We therefore assume for the remainder of the proof that $k \neq -l$. A natural place where to look for an answer is then the quotient group of the free group on $\{a, b\}$ by the normal subgroup generated by the relation $a^k b^l = b^k a^l$, namely the two-generator one-relator group, denoted by $L_{k,l}$, with presentation

$$\langle a, b \mid a^k b^l = b^k a^l \rangle.$$

In fact, by the defining relation of $L_{k,l}$ we have that taking $X = \{a, b\}$ yields

$$|X^k X^l| = |\{a^{k+l}, a^k b^l, b^{k+l}\}| = 3 = 3|X| - 3.$$

Moreover, $L_{k,l}$ is torsion-free, which follows from the fact that a one-relator group has torsion if and only if the relator is a proper power of some other element in the ambient free group, see Proposition 5.18 of [20].

So, we are left to check that the equation

$$a^k b^l a^{-l} b^{-k} = x^t \tag{11}$$

has no solution for t an integer ≥ 2 and x an element in the free group constructed on the set $\{a, b\}$. Suppose the contrary, and let $x = x_1^{u_1} \cdots x_n^{u_n}$, where the u_i are non-zero integers and the x_i belong to $\{a, b\}$, with $x_i^{-1} \neq x_{i+1} \neq x_i$ for each $i = 1, \dots, n-1$. If $y_1^{v_1} \cdots y_m^{v_m}$ is the reduced form of x^t , then $y_1 = x_1$ and $y_m = x_n$. Indeed, the positive power of a reduced word, say w , in a free group is a word which, when reduced to its minimal form, starts and ends with the same letters as w . It follows from (11) that $x_1 = a$ and $x_n = b$, with the result that $m = nt$. Thus, we get $4 = m \geq 2t$, which is possible only if $n = t = 2$. But this yields

$$a^k b^l a^{-l} b^{-k} = a^u b^v a^u b^v$$

for certain non-zero integers u and v . This implies both $u = k$ and $u = -l$, which is impossible since $k \neq -l$. \square

As already mentioned, any linearly orderable group is torsion-free, but not viceversa, as is shown, for instance, by the two-generator one-relator group defined by the presentation $\langle a, b \mid a^2 = b^2 \rangle$, which is actually the fundamental group of the Klein bottle, see Example 1.24 in [16].

The question therefore remains whether or not it is possible to give an extension of Theorem 1 to the case where the group G is linearly orderable (and not just torsion-free). Since we cannot decide whether or not the group $L_{k,l}$, used in the proof above, is linearly orderable, Theorem 2 cannot be immediately extended to linearly orderable groups.

However, the following theorem shows that the answer to this question is negative too, and it represents the main contribution of the paper.

Theorem 3. *Let k and l be positive integers. There then exist a linearly orderable group G and a 2-element set $X \subseteq G$ such that $|k \cdot X + l \cdot X| < 3|X| - 2$.*

The proof is deferred to the next section. In Section 4, we make a first step in the refinement of these results by passing from a 2-element to a 3-element set. At the moment, our constructions do not allow for sets of cardinality larger than 3. This leads us, in Section 5, to raise some questions in this direction.

3. PROOF OF THEOREM 3

We start by recalling the following result by Iwasawa (namely, Lemma 1 in [17]), which gives a practical characterization of orderable groups and will be used below to construct the linearly orderable group (in fact, a semidirect product) required by our proof of Theorem 3.

Lemma 1 (Iwasawa's lemma). *A group G is linearly orderable if and only if there exists a subset P of G , referred to as a positive cone of G , such that:*

- (i) $1 \notin P$,

- (ii) for each $x \in G \setminus \{1\}$ either $x \in P$ or $x^{-1} \in P$,
- (iii) for all $x, y \in P$, $xy \in P$, and
- (iv) if $x \in P$ then $xyx^{-1} \in P$ for all $y \in G$.

Given two groups G and H and a homomorphism $\varphi : H \rightarrow \text{Aut}(G)$, we denote as usual by $G \rtimes_{\varphi} H$ the semidirect product of G by H under φ , that is the (multiplicatively written) group with elements in the set $G \times H$ whose operation is defined by

$$(g_1, h_1)(g_2, h_2) = (g_1\varphi_{h_1}(g_2), h_1h_2)$$

for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$. We recall that the identity in $G \rtimes_{\varphi} H$ is the pair $(1, 1)$, while the inverse of an element $(g, h) \in G \rtimes_{\varphi} H$ is $(\varphi_{h^{-1}}(g^{-1}), h^{-1})$.

With this notation at hand, we have now the following lemma, which provides a practical method for constructing a number of linearly orderable groups. This is essentially a generalization of a result by Conrad (see the first few lines of Section 3 in [8]), where H is assumed to be a subgroup of $\text{Aut}(G)$ and φ is the restriction to H of the trivial automorphism on $\text{Aut}(G)$, that is the identity of $\text{Aut}(\text{Aut}(G))$.

Lemma 2. *Let (G, \preceq_G) and (H, \preceq_H) be linearly ordered groups, and let φ be a homomorphism $H \rightarrow \text{Aut}(G)$. If φ is order-preserving, in the sense that $1 \prec \varphi_h(g)$ for all $g \in G$ and $h \in H$ with $1 \prec g$, then $G \rtimes_{\varphi} H$ is a linearly orderable group.*

Proof. We define P as

$$P = \{(g, h) \in G \times H \text{ with either } 1 \prec h, \text{ or } h = 1, 1 \prec g\}.$$

We shall prove that P is a positive cone of $G \rtimes_{\varphi} H$ by checking the conditions (i)-(iv) in the statement of Iwasawa's lemma.

It is clear by construction that $(1, 1) \notin P$, so (i) is immediate.

As for (ii), let $(g, h) \in P$ and assume for a contradiction that its inverse $(\varphi_{h^{-1}}(g^{-1}), h^{-1})$ is also in P . By the definition of P , $(g, h) \in P$ implies that h must be larger than or equal to 1. But our assumptions give $1 \preceq h^{-1}$, so we must have $h = 1$. It follows that $1 \prec g$ and $1 \prec \varphi_{h^{-1}}(g^{-1}) = \varphi_1(g^{-1}) = g^{-1}$, a contradiction.

Then we come to (iii). Given $(g_1, h_1), (g_2, h_2) \in P$, we compute the product $(g_1, h_1)(g_2, h_2) = (g_1\varphi_{h_1}(g_2), h_1h_2)$ and observe that this is still in P . Indeed, both h_1 and h_2 are larger than or equal to 1, so does their product. If $1 \prec h_1h_2$, we are done. Otherwise, we must have $h_1 = h_2 = 1$. In this case, $g_1\varphi_{h_1}(g_2) = g_1g_2$, which is larger than 1 since both $1 \prec g_1$ and $1 \prec g_2$, by the definition of P .

Finally, we prove (iv): if $(g_1, h_1) \in G \times H$ and $(g_2, h_2) \in P$, then

$$\begin{aligned} (g_1, h_1)(g_2, h_2)(g_1, h_1)^{-1} &= (g_1, h_1)(g_2\varphi_{h_2h_1^{-1}}(g_1^{-1}), h_2h_1^{-1}) \\ &= (g_1\varphi_{h_1}(g_2)\varphi_{h_1h_2h_1^{-1}}(g_1^{-1}), h_1h_2h_1^{-1}). \end{aligned}$$

If $1 \prec h_2$, then $1 \prec h_1 h_2 h_1^{-1}$ and we are done. Otherwise, $h_2 = 1$ and $1 \prec g_2$, with the result that

$$(g_1, h_1)(g_2, h_2)(g_1, h_1)^{-1} = (g_1 \varphi_{h_1}(g_2) g_1^{-1}, 1) \in P,$$

where we use that $1 \prec \varphi_{h_1}(g_2)$ by the fact that φ is order-preserving.

Putting all together, we then have that P is a positive cone of $G \rtimes_{\varphi} H$, and thus the claim follows from Iwasawa's lemma. \square

At this point, we need to introduce some more notation. Specifically, given a subset S of \mathbb{R} , we write $\mathcal{E}[S]$ for the additive subgroup of the real field generated by numbers of the form α^h such that $\alpha \in S$ and $h \in \mathbb{Z}$. In the case when S consists of a unique element, say α , we simply write $\mathcal{E}[\alpha]$ for $\mathcal{E}[\{\alpha\}]$. If α is a positive integer, we call $\mathcal{E}[\alpha]$ the set of α -adic fractions, in that the elements of $\mathcal{E}[\alpha]$ are explicitly given by the rational fractions of the form h/α^t for which $h \in \mathbb{Z}$ and $t \in \mathbb{N}$.

Theorem 4. *Let k be a positive integer and α a positive real number. Consider the set*

$$S = \left\{ \alpha^{k^{-i}} \text{ for } i = 0, 1, 2, \dots \right\}$$

and let φ be the homomorphism $(\mathcal{E}[k], +) \rightarrow \text{Aut}(\mathcal{E}[S], +)$ taking a k -adic fraction u to the automorphism $x \mapsto \alpha^u x$ of $(\mathcal{E}[S], +)$. Finally, let G be the semidirect product

$$G = (\mathcal{E}[S], +) \rtimes_{\varphi} (\mathcal{E}[k], +).$$

The following holds:

- (i) *G is a linearly orderable group.*
- (ii) *Given an integer $l \geq k$, there is a real number $\beta_{k,l} > 0$ satisfying the equation*

$$\sum_{i=k+1}^{k+l} x^{i/k} - \sum_{i=1}^k x^{i/k} = 0.$$

Then, for $\alpha = \beta_{k,l}$ we have

$$e_0^k e_1^l = e_1^k e_0^l$$

where $e_0 = (\alpha^{1/k}, 1/k)$ and $e_1 = (0, 1/k)$ are elements of G .

Proof. Let us first check that φ_u is well-defined as a function $\mathcal{E}[S] \rightarrow \mathcal{E}[S]$ for each $u \in \mathcal{E}[k]$. For, u being a k -adic fraction means that there exist $h \in \mathbb{Z}$ and $t \in \mathbb{N}$ such that $u = h/k^t$. Therefore, using that an element of $\mathcal{E}[S]$ is a real number of the form $\sum_{i=1}^l g_i \alpha^{h_i/k^{t_i}}$ for certain $g_i, h_i \in \mathbb{Z}$ and $t_i \in \mathbb{N}$, we find that

$$\varphi_u(x) = \sum_{i=1}^l g_i \alpha^{h/k^t + h_i/k^{t_i}} = \sum_{i=1}^l g_i \alpha^{s_i/k^{r_i}} \in \mathcal{E}[S],$$

where $r_i = \max(t_i, t)$ and s_i is equal to the integer $k^{r_i-t}h + k^{r_i-t_i}h_i$. It follows that φ is also well-defined as a homomorphism $(\mathcal{E}[k], +) \rightarrow \text{Aut}(\mathcal{E}[S], +)$. In fact, $\varphi_{u+v} = \varphi_u \circ \varphi_v$ for all $u, v \in \mathcal{E}[k]$, and φ_u is bijective, its inverse being φ_{-u} . Lastly, for $u \in \mathcal{E}[k]$ and $x, y \in \mathcal{E}[S]$ we have $\varphi_u(x + y) = \varphi_u(x) + \varphi_u(y)$, that is φ_u is a homomorphism of $(\mathcal{E}[S], +)$.

(i) The claim follows at once from Lemma 2, considering that $(\mathcal{E}[S], +)$ can be linearly ordered by the usual order of \mathbb{R} and $\alpha > 0$ implies that $\varphi_u(x) = \alpha^u x > 0$ for each $u \in \mathcal{E}[k]$ and each positive $x \in \mathcal{E}[S]$.

(ii) Since the polynomial

$$P(x) = \sum_{i=k+1}^{k+l} x^i - \sum_{i=1}^k x^i$$

satisfies $P(0) = 0$, $P'(0) = -1$ and $P(x) \rightarrow +\infty$ as $x \rightarrow +\infty$, it must have one or more positive roots. Let $\beta_{k,l}$ be the k -th power of one of them, chosen arbitrarily.

A straightforward induction shows that for any positive integer j , we have

$$e_0^j = (\alpha^{1/k} + \dots + \alpha^{j/k}, j/k) \text{ and } e_1^j = (0, j/k),$$

whence we get, on the one hand,

$$e_0^k e_1^l = (\alpha^{1/k} + \dots + \alpha^{k/k}, 1)(0, l/k) = (\alpha^{1/k} + \dots + \alpha^{k/k}, 1 + l/k),$$

and on the other hand,

$$e_1^k e_0^l = (0, 1)(\alpha^{1/k} + \dots + \alpha^{l/k}, l/k) = (\alpha^{1+1/k} + \dots + \alpha^{1+l/k}, 1 + l/k).$$

Thus, $e_0^k e_1^l = e_1^k e_0^l$ since $\alpha = \beta_{k,l}$ satisfies $P(\alpha) = 0$. □

Taking $X = \{e_0, e_1\}$ in Theorem 4, we obtain a 2-element set such that

$$|X^{\cdot k} X^{\cdot l}| = 3 = 3|X| - 3.$$

Noticing that we can always reverse the roles of k and l , we thus have the following:

Corollary 1. *Let k and l be positive integers. There exist a linearly orderable group G and a set $X \subseteq G$ of cardinality 2 such that $|X^{\cdot k} X^{\cdot l}| = 3 = 3|X| - 3$.*

This result is enough to conclude our proof of Theorem 3.

4. EXTENDING THEOREM 3

Based on Theorem 3 it is somewhat natural to ask whether it is possible to construct linearly orderable groups where to find sets X of any possible size such that $|k \cdot X + l \cdot X| < 3|X| - 2$ for some non-zero integers k and l . In our final result, we show that this is actually the case with a 3-element set.

Theorem 5. *Let k and r be positive integers, and let α be a positive real number. Consider the set*

$$S = \left\{ \alpha^{k^{-i}} \text{ for } i = 0, 1, 2, \dots \right\}.$$

Define H to be the direct product of r copies of $(\mathcal{E}[S], +)$, and let

$$G = H \rtimes_{\varphi} (\mathcal{E}[k], +),$$

where φ is the homomorphism $(\mathcal{E}[k], +) \rightarrow \text{Aut}(H)$ sending a k -adic fraction u to the automorphism $(x_1, \dots, x_r) \mapsto (\alpha^u x_1, \dots, \alpha^u x_r)$ of H . The following holds:

- (i) *G is a linearly orderable group.*
- (ii) *Let e_i denote, for $i = 0, \dots, r$, the $(r+1)$ -tuple of G whose $(r+1)$ -th component is $1/k$, whose i -th component is $\alpha^{1/k}$ if $i \neq 0$, and all of whose other components are zero. Moreover, let l be an integer $\geq k$ and assume $\alpha = \beta_{k,l}$, where $\beta_{k,l}$ is defined as in Theorem 4, point (ii). Then,*

$$e_i^k e_j^l = e_j^k e_i^l$$

for all $i, j = 0, 1, \dots, r$, and hence

$$|X^{\cdot k} X^{\cdot l}| = 6 = 3|X| - 3$$

for $r \geq 2$ and $X = \{e_0, e_1, e_2\}$.

Proof. We should first check that φ is well-defined as a homomorphism from $(\mathcal{E}[k], +)$ to $\text{Aut}(H)$, but this boils down to the same kind of verification as in the proof of Theorem 4, so we can move on.

(i) The group H can be linearly ordered by the natural lexicographic order on its r components, and accordingly φ is order-preserving. Thus G is a linearly orderable group by Lemma 2.

(ii) Denote by ψ the homomorphism $(\mathcal{E}[k], +) \rightarrow \text{Aut}(\mathcal{E}[S], +)$ taking an k -adic fraction u to the automorphism $x \mapsto \alpha^u x$ of $(\mathcal{E}[S], +)$. Then for each $h = 1, \dots, r$ let π_h be the projection homomorphism

$$G \rightarrow (\mathcal{E}[S], +) \times_{\psi} (\mathcal{E}[k], +) : (x_1, \dots, x_r, u) \rightarrow (x_h, u).$$

This is clearly a surjective homomorphism, and its restriction to the subgroup of G consisting of those $(r+1)$ -tuples (x_1, \dots, x_r, u) such that $x_j \neq 0$ for some $1 \leq j \leq r$ only if $j = h$ is an isomorphism. Therefore, we find that two elements ξ and ζ of G are equal if and only if

$$\pi_h(\xi) = \pi_h(\zeta) \text{ for all } h = 1, \dots, r.$$

With this in hand, fix $i, j = 0, 1, \dots, r$. We have to prove that $e_i^l e_j^k = e_j^l e_i^k$. For, it follows from the above that this is equivalent to

$$\pi_h(e_i)^l \pi_h(e_j)^k = \pi_h(e_j)^l \pi_h(e_i)^k$$

for all $h = 1, \dots, r$ (here we use that π_h is a homomorphism), which in turn is immediate by Theorem 4, since $\pi_h(e_i) = \pi_h(e_j) = (\alpha^{1/k}, 1/k)$ for $i, j \geq 1$ and $\pi_h(e_0) = (0, 1/k)$. \square

By considering the set $X = \{e_0, e_1, \dots, e_{r-1}\}$ in Theorem 5, we obtain the following corollary.

Corollary 2. *Let k, l and r be positive integers. There exist a linearly orderable group G and a set $X \subseteq G$ with $|X| = r$ such that $|X^k X^l| = \binom{r+1}{2}$.*

The special case where $r = 3$ is of particular interest.

Corollary 3. *Let k and l be positive integers. There exist a linearly orderable group G and a set $X \subseteq G$ with $|X| = 3$ such that $|X^k X^l| = 6 = 3|X| - 3$.*

5. SOME QUESTIONS FOR FURTHER RESEARCH

For a group G and non-zero integers k, l and $r \geq 1$, let us denote by

$$\chi_G(k, l, r)$$

the minimal possible cardinality of a sumset of the form $X^k X^l$ for a set $X \subseteq G$ with $|X| = r$. Immediate bounds for this function are

$$r \leq \chi_G(k, l, r) \leq r^2.$$

The lower inequality is in general sharp: it is enough to consider groups containing a cyclic subgroup of order r . However, it can be improved in a number of cases by using, for instance, a Kneser type or Cauchy-Davenport type theorem.

Based on the above, it is then natural to define, for \mathcal{G} a given class of groups,

$$\chi^{\mathcal{G}}(k, l, r) = \inf_{G \in \mathcal{G}} \chi_G(k, l, r).$$

In this paper, we have especially investigated the case when \mathcal{G} is either the class **TF** of torsion-free groups, or the class **LO** of linearly orderable groups. Using **LO** \subsetneq **TF**, (8) and the fact that $(\mathbb{Z}, +)$ is an element of **LO** yields

$$2r - 1 \leq \chi^{\text{TF}}(k, l, r) \leq \chi^{\text{LO}}(k, l, r) \leq \chi_{(\mathbb{Z}, +)}(k, l, r) \leq (|k| + |l|)r - (|k| + |l| - 1). \quad (12)$$

The last upper bound follows from considering $X = \{0, 1, \dots, r - 1\}$.

If $|k| = |l| = 1$, (12) is in fact a series of equalities. In any other case, we must have $|k| + |l| \geq 3$ and the upper bound we obtain from (12) is never better than $3r - 2$. This bound is improved by Theorems 4 and 5 since these results, when combined with equation (12), read as

$$\chi^{\text{TF}}(k, l, 2) = \chi^{\text{LO}}(k, l, 2) = 3 \quad \text{and} \quad 5 \leq \chi^{\text{TF}}(k, l, 3) \leq \chi^{\text{LO}}(k, l, 3) \leq 6$$

for any positive integers k and l . Corollary 3 provides a quadratic bound in r independent from k and l , namely $r(r + 1)/2$. But unfortunately, this is smaller

than the linear upper bound in (12) only for small values of r . In particular, we get a better bound than $3r - 2$ only if $r = 2$ or 3 .

Although the situation is clear for $r = 2$, even the question of which is the exact value of $\chi^{\text{LO}}(k, l, 3) \in \{5, 6\}$ remains open. It is not difficult to see that the answer is 5 if and only if there exist a linearly orderable group G and elements $x, y, z \in G$ such that (i) $x \prec y \prec z$, (ii) $x^k y^l = y^k x^l$, (iii) $x^k z^l = z^k x^l = y^{k+l}$, and (iv) $y^k z^l = z^k y^l$, but this looks challenging to investigate even in the basic case, say, when $k = 1$ and $l = 2$.

A related question is as follows: Let $L^{(r)}$ be the free group on r variables, say x_1, \dots, x_r . We denote by $L_{k,l}^{(r)}$ the quotient group of $L^{(r)}$ by the normal subgroup generated by the relations $x_i^k x_j^l = x_j^k x_i^l$ as i and j range in the interval $\{1, \dots, r\}$. When $r = 2$, this is the two-generator one-relator group considered at the end of Section 2. Are the $L_{k,l}^{(r)}$ linearly orderable groups? Are they torsion-free? If $r = 2$, one can see using von Dyck's theorem (namely, Theorem 2.2.1 in [27]) that there exists an epimorphism $\vartheta : L_{k,l}^{(2)} \rightarrow G$, the group constructed in Theorem 4, mapping x_1 to $(\alpha, 1)$ and x_2 to $(0, 1)$. We ask if ϑ is actually an isomorphism. If the answer to this question were yes, this would imply that $L_{k,l}^{(2)}$ is linearly orderable.

More generally, let \mathcal{R} be a set of independent relations on the r variables of the free group $L^{(r)}$, each being of the form

$$x_i^k x_j^l = x_u^k x_v^l$$

where i, j, u and v belong to $\{1, \dots, r\}$. We denote by $L_{\mathcal{R}}^{(r)}$ the quotient group of $L^{(r)}$ by the normal subgroup generated by the set of relations \mathcal{R} . How large can \mathcal{R} be if we require that $L_{\mathcal{R}}^{(r)}$ is linearly orderable or torsion-free? Since each of the above relations makes the cardinality of the sum $X^{\cdot k} X^{\cdot l}$, where X is the set $\{x_1, \dots, x_r\}$, decrease by one, looking for a large \mathcal{R} is tightly related to having good upper bounds on $\chi^{\text{TF}}(k, l, r)$ and $\chi^{\text{LO}}(k, l, r)$ and could help to understand the behaviour of these functions.

ACKNOWLEDGEMENTS

The second-named author is grateful to Yves de Cornulier for a useful observation which eventually led to the formulation of Lemma 2.

REFERENCES

- [1] A. Balog, and G. Shakan, *On the sum of dilations of a set*, Acta Arith. **164** (2014), 153–162.
- [2] ———, *Sum of dilates in vector spaces*, preprint ([arXiv:1410.8614](https://arxiv.org/abs/1410.8614)), last updated: Oct 31, 2014.
- [3] K. J. Böröczky, P. P. Pálffy, and O. Serra, *On the cardinality of sumsets in torsion-free groups*, Bull. Lond. Math. Soc. **44**, No. 5 (2012), 1034–1041.

- [4] G. Baumslag and D. Solitar, *Some two-generator one-relator non-Hopfian groups*, Bull. Amer. Math. Soc. **68** (1962), 199–201.
- [5] B. Bukh, *Sums of dilates*, Combin. Probab. Comput. **17**, No. 5 (2008), 627–639.
- [6] J. Cilleruelo, Y. O. Hamidoune, and O. Serra, *On sums of dilates*, Combin. Probab. Comput. **18**, No. 6 (2009), 871–880.
- [7] J. Cilleruelo, M. Silva, and C. Vinuesa, *A sumset problem*, J. Comb. Number Theory **2**, No. 1 (2010), 79–89.
- [8] P. Conrad, *Non-abelian ordered groups*, Pacific J. Math. **9**, No. 1 (1959), 25–41.
- [9] P. Dehornoy, I. Dynnikov, D. Rolfsen, and B. Wiest, *Why are braids orderable?*, Panoramas & Synthèses **14**, Soc. Math. France, 2002.
- [10] G. A. Freiman, M. Herzog, P. Longobardi, and M. Maj, *Small doubling in ordered groups*, J. Austral. Math. Soc. **96**, No. 3 (2014), 316–325.
- [11] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, and Y. V. Stanchescu, *Inverse problems in additive number theory and in non-abelian group theory*, European J. Combin. **40** (2014), 42–54.
- [12] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne, and Y. V. Stanchescu, *Small doubling in ordered groups: generators and structure*, preprint ([arXiv:1501.01838](https://arxiv.org/abs/1501.01838)), last updated: Jan 8, 2015.
- [13] M. Z. Garaev, *An explicit sum-product estimate in \mathbb{F}_p* , Int. Math. Res. Not. **11** (2007), Art. ID rnm035.
- [14] Y. O. Hamidoune and A. Plagne, *A generalization of Freiman’s $3k - 3$ theorem*, Acta Arith. **103**, No. 2 (2002), 147–156.
- [15] Y. O. Hamidoune and J. Rué, *A lower bound for the size of a Minkowski sum of dilates*, Combin. Probab. Comput. **20**, No. 2 (2011), 249–256.
- [16] A. Hatcher, *Algebraic topology*, Cambridge University Press, 2002.
- [17] K. Iwasawa, *On linearly ordered groups*, J. Math. Soc. Japan **1** (1948), 1–9.
- [18] J. H. B. Kemperman, *On complexes in a semigroup*, Indag. Math. **18** (1956), 247–254.
- [19] S. Konyagin and I. Łaba, *Distance sets of well-distributed planar sets for polygonal norms*, Israel J. Math **152** (2006), 157–179.
- [20] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer-Verlag, 1977.
- [21] A. I. Malcev, *On ordered groups*, Izv. Akad. Nauk. SSSR Ser. Mat. **13** (1948), 473–482.
- [22] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Vol. 165 in the Graduate Texts in Mathematics series, Springer, 1996.
- [23] M. B. Nathanson, *Inverse problems for linear forms over finite sets of integers*, J. Ramanujan Math. Soc. **23**, No. 2 (2008), 151–165.
- [24] B. H. Neumann, *On ordered groups*, Amer. J. Math. **71** (1949), 1–18.
- [25] A. Plagne, *Sums of dilates in groups of prime order*, Combin. Probab. Comput. **20**, No. 6 (2011), 867–873.
- [26] G. F. Pontiveros, *Sums of Dilates in \mathbb{Z}_p* , Combin. Probab. Comput. **22**, No. 2 (2013), 282–293.
- [27] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, 1982.
- [28] D. Rolfsen and J. Zhu, *Braids, orderings and zero divisors*, J. Knot Theory Ramifications **7**, No. 6 (1998), 837–841.
- [29] G. Shakan, *A bound for the size of the sum of dilates*, preprint ([arXiv:1402.4721](https://arxiv.org/abs/1402.4721)), last updated: Jan 14, 2014.
- [30] S. Tringali, *Cauchy-Davenport type theorems for semigroups*, to appear in Mathematika ([arXiv:1307.8396](https://arxiv.org/abs/1307.8396)).

- [31] ———, *Small doubling in ordered semigroups*, Semigroup Forum **90**, No. 1 (2015), 135–148.

CENTRE DE MATHÉMATIQUES LAURENT SCHWARTZ, ÉCOLE POLYTECHNIQUE, 91128 PALAISEAU
CEDEX, FRANCE

E-mail address: `plagne@math.polytechnique.fr`

URL: `http://www.math.polytechnique.fr/~plagne/`

SCIENCE PROGRAM, TEXAS A&M UNIVERSITY AT QATAR, EDUCATION CITY, PO BOX
23874 DOHA, QATAR

E-mail address: `salvo.tringali@gmail.com`

URL: `http://www.math.polytechnique.fr/~tringali/`